CMP Algorithms, CMP Updates, and Lightweight CMP Profile

draft-ietf-lamps-cmp-algorithms-01

draft-ietf-lamps-cmp-updates-06

draft-ietf-lamps-lightweight-cmp-profile-04

Hendrik Brockhaus, Steffen Fries, David von Oheimb

IETF 109 – LAMPS Working Group

New I-D on CMP Algorithms

As proposed during IETF 108 a new draft on CMP Algorithms was submitted

Current content structure

2. Message Digest Algorithms
3. Signature Algorithms
4. Key Management Algorithms
    1. Key Agreement Algorithms
    2. Key Transport Algorithms
    3. Symmetric Key-Encryption Algorithms
    4. Key Derivation Algorithms
5. Content Encryption Algorithms
6. Message Authentication Code Algorithms

CMP Algorithms - Status and ToDos

Section 2. Message Digest Algorithms

- Currently SHA2 (RFC5754) family is listed
- I plan to add SHAKE (RFC8702)
- What is the opinion of the WG? Are there further hash algorithms to be added? Is BLAKE2 still in focus of the IETF?

Section 5. Content Encryption Algorithms → AES

- Currently AES-CCM and AES-GCM (RFC5084) are listed
- I could add AES-CBC (RFC3565) and ChaCha20-Poly1305 (RFC8103)
- What is the opinion of the group?

Section 6. Message Authentication Code Algorithms

- Currently PasswordBasedMac (RFC4211), PBMAC1 (RFC8018), DHBasedMac (RFC4211), and SHA2-based HMAC (RFC4231) are listed
- I plan to add AES-GMAC (draft-housley-lamps-cms-aes-mac-alg) and SHAKE-based KMAC (RFC8702)
- What is the opinion of the WG? Are there further MAC algorithms to be added? What about AES-CMAC?

CMP Algorithms - Status and ToDos

I did not look deeper into these sections so far.

Section 3. Signature Algorithms

- Currently DSA, RSA, and ECDSA with SHA2 (RFC5754) and RSASSA-PSS (RFC4056) are listed
- For ECDSA, should we list specific curves to support, e.g., secp256r1, Curve 22519?

Section 4. Key Management Algorithms

4.1 Key Agreement Algorithms

- Currently Diffie-Hellmann (RFC3370) and ECDH (RFC5753) are listed
- Should we list static-static (EC)DH variants?

4.2 Key Transport Algorithms

- Currently PKCS#1 V1.5 (RFC3370) and RSAES-OAEP (RFC3560) is listed

4.3 Symmetric Key-Encryption Algorithms

- Currently AES Key Wrap (RFC3565) is listed

4.4 Key Derivation Algorithms

- Currently PBKDF2 (RFC8018) is listed

What is the opinion of the WG? Any Feedback is welcome!

Activities since IETF 108 on CMP Updates

All issues from IETF 108 and subsequent discussion on the mailing list were addressed

- Updated Section 2.4 to add the AsymmetricKey Package structure to transport a newly generated private key
- Added Section 2.6 and Section 2.7 to clarify the usage of these general messages types with EC curves
- Added Sections 2.9, 2.10, and 2.11 to add new general message types id-it-caCerts, id-it-rootCaKeyUpdate, and id-it-certReqTemplate used in the Lightweight CMP Profile
- Changed in Section 2.10 to use controls as specified in CRMF instead of rsaKeyLeng
- Updated Section 2.13 to add new id-it IDs, id-regCtrl IDs and /.well-known/cmp
- Added Section 2.16 to update RFC4210 Appendix D.2 with the reference to CMP Algorithms
- Added Section 3 to document the changes to RFC 6712 [RFC6712] regarding URI discovery and using the path-prefix of '/.well-known/' and changed wording after review by Martin Peylo
- Added Appendix A.1 with an updated 1988 ASN.1 module and Appendix A.2 with an updated 2002 ASN.1 module

Questions regarding Root CA Certificates Update - 1

2.10. New Section 5.3.19.15 - Root CA Certificates Update

Currently the request for an root CA certificate is unspecific and the response contains only one update triple

```
GenMsg:     {id-it 18}, < absent >
GenRep:     {id-it 18}, RootCaKeyUpdateContent | < absent >

RootCaKeyUpdateContent ::= SEQUENCE {
   newWithNew         CMPCertificate
   newWithOld    [0]  CMPCertificate OPTIONAL,
   oldWithNew    [1]  CMPCertificate OPTIONAL
   }
```

In case the PKI supports more than one Root CA, how to specify which update to respond

Questions regarding Root CA Certificates Update - 2

Proposal for Root CA Certificates Update

- Add content in the request message, e.g., the oldWithOld or a kind of template identifier

Questions regarding new Certificate Request Template - 1

2.11. New Section 5.3.19.16 - Certificate Request Template

Currently the request for an certificate request template is unspecific and the response contains only one template

```
GenMsg:    {id-it 19}, < absent >
GenRep:    {id-it 19}, CertReqTemplateContent | < absent >
CertReqTemplateContent ::= SEQUENCE {
   certTemplate           CertTemplate,
   controls               Controls OPTIONAL }
Controls ::= SEQUENCE SIZE(1..MAX) OF AttributeTypeAndValue
id-regCtrl-algId OBJECT IDENTIFIER ::= { id-regCtrl TBD3 }
  AlgIdCtrl ::= AlgorithmIdentifier
id-regCtrl-rsaKeyLen OBJECT IDENTIFIER ::= { id-regCtrl TBD4 }
  RsaKeyLenCtrl ::= Integer
```

Most likely the PKI supports more than one Certificate profile, how to specify which template to respond to

Questions regarding new Certificate Request Template - 2

Most likely the PKI supports more than one Certificate profile, how to specify which template to respond to.

Is there any best practice to specify/address (also via several hops) the certificate template that should be used for processing a certificate request?

Proposal for addressing certificate profiles in Certificate Requests and Certificate Request Template general messages as fallback.

- Register a new id-it InfoTypeValue for use in PKIHeader.generalInfo?

Further questions on CMP Updates

- We propose to use new id-regCtrl AttibuteTypeValues in the context of Certificate Request Template general message. Is it OK to reuse the type Controls as specified in RFC 4211 Section 6 also for algorithm preferences?
- Should we use "GET /.well-known/cmp" or "GET /.well-known" only for discovering CMP related HTTP endpoints? This maybe synchronized with BRSKI(-AE).
- Does this draft also updates RFC 5912, as we update the 2002 ASN.1 module from RFC 5912?

Remaining ToDos for CMP Updates

- Guidance is appreciated on how to do the discovery, either using "GET /.well-known/cmp" or "GET /.well-known" only
- Define and register OID id-regCtrl-algId and id-regCtrl-rsaKeyLen at IANA (pre-registration would be appreciated)
- Update description of id-kp-cmcCA and id-kp-cmcRA at IANA
- Polish wording and correct typos

Any further feedback is welcome!

Activities since IETF 108 on Lightweight CMP Profile

All issues from IETF 108 and subsequent discussion on the mailing list were addressed

- Deleted normative text sections on algorithms and refer to CMP Algorithms and CRMF Algorithm Requirements Update instead
- Updated Section 1.4 regarding interoperability with [UNISIG-Subset137]
- Changed Section 2.3 to a tabular layout to enhanced readability
- Updated Section 4.1.6 to use the AsymmetricKey Package structure to transport a newly generated private key
- Updated Section 4 due to the definition of the new ITAV OIDs in CMP Updates
- Updated Section 4.4.4 to utilize id-regCtrl instead of rsaKeyLen
- Deleted the section on definition and discovery of HTTP URIs and copied the text to the HTTP transport section and to CMP Updates Section 3.2
- Updated Section 5.1.2 and Section 5.1.3 by adding explanation on using nested messages when a protection by the RA is required
- Deleted the ASN.1 module after moving the new OIDs id-it-caCerts, id-it-rootCaKeyUpdate, and id-it-certReqTemplate to CMP Updates

Remaining ToDos for Lightweight CMP Profile

- Update Section 4.4.2 and 4.4.3 based on outcome of the previous discussion on new CMP support messages
- We are looking for a suitable TLS cipher suite for use with pre-shared secrets or passwords due to limited support of TLS-SRP, e.g., in JSSE. Any suggestions?
- Update of example for CertReqTemplate is required
- Polish wording and correct typos

Any further feedback is welcome!